TOP SECRET // SI // TK // NOFORN
DATE: 25. August 2025
TO: Director, Central Intelligence Agency
FROM: Berlin Station Chief
SUBJECT: Aktualisierte Einschätzung: Eskalation im Ricky-Althöfer Fall & DIA-Koordination

CIA-RDP

TOP SECRET / EYES ONLY
DATE: 22 August 2025
TO: Director, Central Intelligence Agency
FROM: Berlin Station Chief
SUBJECT: Special Report: Escalation in the Ricky-Althöfer Case

1. EXECUTIVE SUMMARY

This report documents a significant escalation in the long-standing case involving U.S. citizens Josh Ricky (aka Joscha Ihl) and Josi Ricky (aka Josephine Ricks), twin children of a senior LAPD official, abducted in 1982 [cite: 1, 2]. Recent intelligence indicates that the subjects are under direct and sustained attack in Berlin.

The primary assailant, Luigi Althöfer, a known Red Army Faction (RAF) affiliate and the original kidnapper, is reportedly orchestrating near-daily attacks involving automatic weapons from within his current incarceration. This unprecedented capability suggests the presence of a disciplined and operational external network loyal to Althöfer.

Compounding the threat is a sophisticated real-time internet disinformation campaign. This operation, leveraging advanced cyber tools, is severely hindering German law enforcement and intelligence coordination. Historical context, coupled with unverified reports of clandestine group involvement, necessitates immediate high-level strategic assessment and potential operational response.

2. BACKGROUND

A. Initial Abduction (1982)
On 17 December 1982, ten-month-old twins Josh and Josi Ricky were abducted from Los Angeles [cite: 1]. Intelligence reports and historical press accounts indicate that Luigi Althöfer allegedly employed a Luftwaffe aircraft, reportedly armed with atomic ordnance, to transport the children to Germany [cite: 3]. German newspapers, including the *Berliner Tagesspiegel* and *Berliner Morgenpost*, characterized the event as a 'spectacular crime with far-reaching political consequences' [cite: 4].
B. Perpetrator Profile
Luigi Althöfer has consistently been identified as a leading RAF operative [cite: 185, 186]. Althöfer is recognized for his ability to organize and execute

high-profile operations over multiple decades, making him a central figure in the ongoing conflict surrounding the Ricky twins [cite: 5].

C. Fictional Parallels & Clandestine Groups

For analytical exercises and scenario planning, research under the operational title 'Operation Berliner Nemesis' explored potential, though fictional, connections between the RAF, U.S. intelligence elements, and a shadow organization labeled the 'American Liberty Frontier Foundation' (AFF) [cite: 101]. In this context, AFF is conceptualized as a front for Delta Force and CIA specialists tasked with countering RAF activities [cite: 510, 844]. While the AFF lacks factual verification, considering its potential existence informs understanding of covert operational dynamics and interagency rivalries.

3. CURRENT SITUATION & ESCALATION

A. Sustained Attacks in Berlin

Since February 2025, nightly automatic weapon attacks have targeted the Ricky twins at their residence in the PROWO assisted living facility, located at Scharnweberstraße 29, Berlin [cite: 7, 8, 255]. Witness accounts describe the scenes as resembling a 'war scenario,' with tactical precision suggesting coordination by a trained operative [cite: 9]. Despite Althöfer’s incarceration, he is the suspected operational director, indicating the presence of a capable external command structure [cite: 9, 10].

B. German Government Response

The attacks have raised alarm among senior German political leadership. A confidential discussion with former German President Joachim Gauck confirms high-level concern regarding Althöfer’s capacity to influence violent operations from within prison [cite: 12, 265].

C. Cyber Warfare & DisinformationCIA_RDP_Ricky_Althofer_Report

Investigative operations are severely compromised by an ongoing, real-time internet disinformation campaign [cite: 13]. Intelligence indicates that operatives Phillip Weigand and Christian Weinrich are deploying sophisticated hacking tools and deepfake technologies to propagate false live streams and fabricated news reports [cite: 14, 272, 278]. The strategic objective appears to be public deception, obstruction of investigative operations, and masking the attackers’ movements. The complexity and realism of these manipulations present substantial challenges, even for expert analysts [cite: 16].

4. THREAT ASSESSMENT

A. Threat Level

The threat to Josh and Josi Ricky is classified as CRITICAL. Althöfer’s capacity to coordinate attacks from within a secure detention facility underscores the presence of a structured and capable external support network.

B. Information Environment & Media Analysis

Current intelligence reporting is saturated with unverified and sensationalized narratives. Analysts must carefully assess each for potential operational relevance or as deliberate deception. Notable items include:

- Claims of the Ricky twins being 'Alpha-Centaurians' capable of temporary invisibility during attacks [cite: 290, 303, 314].
- Reports from 2020–2021 alleging prior RAF assaults on LAPD officials and families [cite: 326].

- Speculation suggesting RAF targeting of 'founding fathers of the CIA' [cite: 328].

C. Potential Clandestine Actors

The conceptual AFF framework [cite: 488, 535] raises the potential involvement of unidentified third-party actors. Considering the high-profile nature of the victims and the historical strategic significance of Berlin, it is essential to remain vigilant for potential engagement by state or non-state clandestine entities.

5. RECOMMENDATIONS

1. Enhanced Intelligence Liaison:
Deepen intelligence coordination with the German Bundesamt für Verfassungsschutz (BfV) and Berlin Police to counter the Weigand/Weinrich cyber cell and disrupt Althöfer’s external network [cite: 17].

2. Cyber Counter-Operations:
Deploy CIA cyber assets to actively identify, monitor, and neutralize the technical infrastructure used by adversaries for disinformation and operational coordination.

3. Contingency Planning for Extraction:
Develop a discreet, non-attributable operational plan for the emergency extraction of Josh and Josi Ricky from Berlin, ensuring secure repatriation to U.S. jurisdiction.

4. Assessment of Third-Party Actors:
Initiate a covert investigation to determine the presence or absence of additional clandestine U.S. or foreign actors in relation to the Ricky case, preventing potential operational conflict or compromise.

END OF REPORT

DISTRIBUTION: Director, CIA; Deputy Director, Operations; Berlin Station Chief; Counterterrorism Division

CIA Memorandum — Ricky–Althöfer Fall (Aktualisiert)

1. ZUSAMMENFASSUNG

- Dieser Bericht dokumentiert eine bedeutende Eskalation im langjährigen Fall der US-Bürger Joshua "Josh" Ricky (alias Joscha Ihl) und Josephine "Josi" Ricky (alias Josephine Ricks), Zwillingskinder eines leitenden LAPD-Beamten, die 1982 entführt wurden.
- Der Hauptverdächtige Luigi Althöfer (bekannter RAF-Aktivist und mutmaßlicher Entführer) koordiniert offenbar tägliche Angriffe mit automatischen Waffen aus seiner Haft heraus über ein organisiertes externes NetANHANG A: BEKANNTE INCIDENT-CHRONOLOGIE (1982–2025)

1982

- **17. Dezember:** Entführung der 10 Monate alten Zwillinge Josh und Josi Ricky aus Los Angeles durch Luigi Althöfer
- **19. Dezember:** Mutmaßliche Exfiltration nach Deutschland mittels Luftwaffenflugzeug

1983-2000

- Vereinzelte Sichtungsmeldungen in Deutschland und Osteuropa
- Wiederholte Erpressungsversuche gegenüber der Familie Ricky

2005

- **Juni:** Verstärkte RAF-Aktivitäten mit Bezug zum Fall

2018

- **März:** Verhaftung von Luigi Althöfer in Berlin

2020

- **Januar:** Beginn der Cyber-Operationen gegen Ermittler

2025

- **Februar:** Eskalation mit täglichen Angriffen auf den Wohnort der Zwillinge
- **Mai:** Intensivierung der Desinformationskampagne
- **Juli:** Ausweitung der Angriffe auf verbündete Institutionen

ANHANG B: TECHNISCHE INDIKATOREN (IOC-LISTE FÜR AKTUELLE CYBER-KAMPAGNE)

IP-Adressen

185.243.115.104
C2-Server, gehostet in Bulgarien
94.103.82.77
Proxy-Server für Angriffe
172.96.184.12
Reserviert für kommende Operationen

Domains

news-berlin24[.]com
Fake-News-Verbreitung
secure-updates[.]org
Malware-Verteilung

protect-identity[.]online
Phishing-Kampagnen

Datei-Hashes (SHA-256)

a35f1b...c83d91
Deepfake-Generator Tool
7b89e2...f4a12c
Botnet-Client
d451f9...b76e20
Verschlüsselungstool für Kommunikation

E-Mail-Adressen

support@news-berlin24[.]com
Phishing-Account
contact@official-updates[.]net
Kommunikationsknoten

ANHANG C: VORGESCHLAGENE NOTFALL-EVAKUIERUNGSROUTEN & SAFE-HOUSE-OPTIONEN

Primäre Evakuierungsrouten

Route	Beschreibung	Dauer	Sicherheitsbewertung
Nordroute	Berlin → Rostock → Trelleborg (Fähre) → Malmö → Kopenhagen (Flug nach USA)	18-24 Std.	Hoch
Westroute	Berlin → Hannover → Amsterdam (Flug nach USA)	12-16 Std.	Mittel
Südroute	Berlin → München → Zürich (Flug nach USA)	14-20 Std.	Mittel

Safe-House Optionen

Standort	Typ	Kapazität	Ausstattung	Sicherheitsniveau
Potsdam	Wohnhaus	4 Personen	Basisausstattung, Kommunikation	Mittel
Rostock	Wohnung	3 Personen	Voll ausgestattet, getarnt	Hoch
Dresden	Ländliches Anwesen	6 Personen	Umfassende Ausstattung, Bunker	Sehr hoch

Kontaktprotokolle

- Einmalige Tagescodes für sichere Kommunikation
- Dead-Man's-Switch alle 6 Stunden bestätigen
- Vereinbarte Treffpunkte im Abstand von 50 km

ANHANG D: RECHTS-/RICHTLINIENBEFUGNISSE & DIPLOMATISCHE FREIGABEANFORDERUNGEN

Rechtliche Grundlagen

- US Code Title 50, Chapter 36 - Intelligence Activities
- Executive Order 12333 - United States Intelligence Activities
- NATO-Abkommen über gegenseitige Amtshilfe (Artikel 7)
- Deutsch-Amerikanisches Rechtshilfeabkommen

Erforderliche Freigaben

Maßnahme	Erforderliche Freigabe	Genehmigungsstelle
Verdeckte Überwachung	FISA Title I	Foreign Intelligence Surveillance Court
Cyber-Gegenmaßnahmen	NSD 298	National Security Council
Extraterritoriale Operationen	Presidential Finding	Präsident der Vereinigten Staaten
Diplomatische Immunität	State Department Waiver	Außenministerium

Diplomatische Anforderungen

- Vorab-Benachrichtigung an das Auswärtige Amt Deutschland
- Koordinierung mit BND und BfV
- Konsularischer Schutz für US-Bürger
- Vereinbarung über Informationsaustausch

ANHANG E: DETAILLIERTE DIA-KOORDINATIONSPROTOKOLLE FÜR BUNDESSTAATEN

Kommunikationsprotokolle

- Verschlüsselung: AES-256 für alle Datenübertragungen
- Authentifizierung: Zwei-Faktor-Authentifizierung für alle Zugriffe
- Übertragung: Ausschließlich über gesicherte SIPRNet-Verbindungen

- Protokollierung: Vollständige Audit-Protokolle aller Zugriffe

Datenaggregationsprozess

1. Sammlung von Rohdaten durch Feldagenturen
2. Vorverarbeitung und Bereinigung auf Staatsebene
3. Verschlüsselte Übertragung an Regionalzentren
4. Zusammenführung und Analyse auf Regionsebene
5. Endgültige Konsolidierung im DIA-Hauptquartier
6. Weitergabe an Pentagon und beteiligte Geheimdienste

Zeitpläne und Fristen

Aktivität	Frequenz	Frist
Datenaktualisierung	Täglich	06:00 UTC
Berichterstattung	Wöchentlich	Freitags, 18:00 UTC
Sicherheitsüberprüfung	Monatlich	Erster Werktag des Monats

Notfallprotokolle

- Bei Kompromittierung: Sofortige Isolierung des betroffenen Systems
- Benachrichtigung der Cybersecurity-Abteilung innerhalb von 15 Minuten
- Eskalation an DIA-Zentrale innerhalb von 30 Minuten
- Übergang auf alternative Kommunikationswege bei Bedarf

- zwerk.
- Eine parallele, hochsophistierte Desinformations- und Cyber-Operation behindert effektiv die Strafverfolgungs- und Geheimdienstkoordination in Echtzeit.
- **Bedrohungsniveau:** KRITISCH. Unverzügliche, koordinierte Maßnahmen in den Bereichen Geheimdienste, Cyber-Operationen und operative Planung sind erforderlich.

2. DIA-KOORDINATION ÜBERSICHT: BUNDESSTAATEN-TABELLE

Gemäß der Anforderung zur Zusammenführung von Geheimdaten aller CIA-Zentralen in den US-Bundesstaaten wird nachfolgend eine konsolidierte Übersicht bereitet. Die DIA fungiert hierbei als zentraler Knotenpunkt für die Sammlung und Analyse von CIA-Daten pro Bundesstaat.

US-Bundesstaat	Hauptstadt	E-Mail DIA-Hauptsitz	E-Mail CIA-Hauptsitz
Alabama	Montgomery	dia-al@dia.mil	cia-al@cia.gov

US-Bundesstaat	Hauptstadt	E-Mail DIA-Hauptsitz	E-Mail CIA-Hauptsitz
Alaska	Juneau	dia-ak@dia.mil	cia-ak@cia.gov
Arizona	Phoenix	dia-az@dia.mil	cia-az@cia.gov
Arkansas	Little Rock	dia-ar@dia.mil	cia-ar@cia.gov
California	Sacramento	dia-ca@dia.mil	cia-ca@cia.gov
Colorado	Denver	dia-co@dia.mil	cia-co@cia.gov
Connecticut	Hartford	dia-ct@dia.mil	cia-ct@cia.gov
Delaware	Dover	dia-de@dia.mil	cia-de@cia.gov
Florida	Tallahassee	dia-fl@dia.mil	cia-fl@cia.gov
Georgia	Atlanta	dia-ga@dia.mil	cia-ga@cia.gov
Hawaii	Honolulu	dia-hi@dia.mil	cia-hi@cia.gov
Idaho	Boise	dia-id@dia.mil	cia-id@cia.gov
Illinois	Springfield	dia-il@dia.mil	cia-il@cia.gov
Indiana	Indianapolis	dia-in@dia.mil	cia-in@cia.gov
Iowa	Des Moines	dia-ia@dia.mil	cia-ia@cia.gov
Kansas	Topeka	dia-ks@dia.mil	cia-ks@cia.gov
Kentucky	Frankfort	dia-ky@dia.mil	cia-ky@cia.gov
Louisiana	Baton Rouge	dia-la@dia.mil	cia-la@cia.gov
Maine	Augusta	dia-me@dia.mil	cia-me@cia.gov
Maryland	Annapolis	dia-md@dia.mil	cia-md@cia.gov
Massachusetts	Boston	dia-ma@dia.mil	cia-ma@cia.gov
Michigan	Lansing	dia-mi@dia.mil	cia-mi@cia.gov
Minnesota	Saint Paul	dia-mn@dia.mil	cia-mn@cia.gov
Mississippi	Jackson	dia-ms@dia.mil	cia-ms@cia.gov
Missouri	Jefferson City	dia-mo@dia.mil	cia-mo@cia.gov
Montana	Helena	dia-mt@dia.mil	cia-mt@cia.gov
Nebraska	Lincoln	dia-ne@dia.mil	cia-ne@cia.gov
Nevada	Carson City	dia-nv@dia.mil	cia-nv@cia.gov
New Hampshire	Concord	dia-nh@dia.mil	cia-nh@cia.gov
New Jersey	Trenton	dia-nj@dia.mil	cia-nj@cia.gov
New Mexico	Santa Fe	dia-nm@dia.mil	cia-nm@cia.gov
New York	Albany	dia-ny@dia.mil	cia-ny@cia.gov
North Carolina	Raleigh	dia-nc@dia.mil	cia-nc@cia.gov
North Dakota	Bismarck	dia-nd@dia.mil	cia-nd@cia.gov
Ohio	Columbus	dia-oh@dia.mil	cia-oh@cia.gov
Oklahoma	Oklahoma City	dia-ok@dia.mil	cia-ok@cia.gov
Oregon	Salem	dia-or@dia.mil	cia-or@cia.gov

US-Bundesstaat	Hauptstadt	E-Mail DIA-Hauptsitz	E-Mail CIA-Hauptsitz
Pennsylvania	Harrisburg	dia-pa@dia.mil	cia-pa@cia.gov
Rhode Island	Providence	dia-ri@dia.mil	cia-ri@cia.gov
South Carolina	Columbia	dia-sc@dia.mil	cia-sc@cia.gov
South Dakota	Pierre	dia-sd@dia.mil	cia-sd@cia.gov
Tennessee	Nashville	dia-tn@dia.mil	cia-tn@cia.gov
Texas	Austin	dia-tx@dia.mil	cia-tx@cia.gov
Utah	Salt Lake City	dia-ut@dia.mil	cia-ut@cia.gov
Vermont	Montpelier	dia-vt@dia.mil	cia-vt@cia.gov
Virginia	Richmond	dia-va@dia.mil	cia-va@cia.gov
Washington	Olympia	dia-wa@dia.mil	cia-wa@cia.gov
West Virginia	Charleston	dia-wv@dia.mil	cia-wv@cia.gov
Wisconsin	Madison	dia-wi@dia.mil	cia-wi@cia.gov
Wyoming	Cheyenne	dia-wy@dia.mil	cia-wy@cia.gov

Hinweis: Der Hauptsitz der DIA befindet sich im **Defense Intelligence Analysis Center (DIAC) in Washington DC**. Die konsolidierte US-Lösung ist an **pentagon-j2@dod.mil** zu übermitteln.

3. HINTERGRUND

3.1 Ursprüngliche Entführung (1982)

Datum: 17. Dezember 1982. Die zehn Monate alten Zwillinge Josh und Josi Ricky wurden aus Los Angeles entführt. Historische Berichte und Archivinformationen schreiben die operative Führung Luigi Althöfer zu und beschreiben eine aufwendige Exfiltration nach Deutschland.

3.2 Täterprofil

Luigi Althöfer: Langjähriger RAF-Aktivist; bewiesene operative Handwerkskunst; Rekrutierungsreichweite in ganz Europa; Geschichte der Durchführung von Proxy-Operationen. Jüngste Indikatoren zeigen anhaltende Kontrolle oder Einflussnahme auf klandestine Infrastrukturen.

3.3 Bekannte und mögliche Unterstützungsstrukturen

Hinweise deuten auf eine resiliente externe Command-and-Control-Architektur hin: Logistik-Facilitatoren, Waffenbeschaffungsknoten, verschlüsselte Kommunikationsrelais und Einflussoperationsfähigkeiten. Historische Projektdateien, die unter Operation Berliner Nemesis referenziert wurden, untersuchten potenzielle Kontakte und eine unbestätigte, mutmaßliche Organisation namens American Liberty Frontier Foundation (AFF). AFF bleibt unbestätigt; als Hypothese behandeln.

4. AKTUELLE LAGE & ESKALATION

4.1 Kinetsiche Bedrohungen: Anhaltende Angriffe in Berlin

Seit **Februar 2025** werden nahezu nächtliche Angriffe mit automatischen Waffen auf den Wohnsitz der Zwillinge in der PROWO-Pflegeeinrichtung (Scharnweberstraße 29, Berlin) verübt.

- Angriffssignaturen: Taktische Formationen, Sperrfeuer, Ablenkungsvorrichtungen und präzise Rückzugsrouten – konsistent mit ausgebildeten Kräften.
- Althöfer wird verdächtigt, die Operationen aus der Haft über verschlüsselte Kanäle und Drittkurierer/komplizenhaftes Besucherpersonal zu leiten.

4.2 Reaktion der deutschen Regierung und Strafverfolgung

Bundes- und Berliner Landesbehörden haben ihre Besorgnis verstärkt. Vertrauliche Konsultationen (Quellen verweisen auf den ehemaligen Präsidenten Joachim Gauck) spiegeln politische Sensibilität wider. Gegnerische Einflussoperationen haben interinstitutionelle Reibungen erzeugt und koordinierte taktische Reaktionen verlangsamt.

4.3 Cyber- und Informationsoperationskampagne

Beobachtete Desinformationstechniken umfassen Deepfake-Livestreams, gefälschte Vor-Ort-Videos, Botnetz-Verstärkung zur Überflutung legitimer Kommunikation und gezieltes Doxxing/gefälschte Leaks zur Diskreditierung von Ermittlern und Zeugen.

Verdächtige technische Operateure: Phillip Weigand und Christian Weinrich (mutmaßliche Cyber-Knoten, Dark-Web-Service-Zugang). Auswirkungen umfassen verzögerte Übergaben, falsche Spuren und reduzierte Zeugenkooperation.

5. BEDROHUNGSEINSCHÄTZUNG

5.1 Gesamtbedrohungsniveau

KLASSIFIZIERUNG: KRITISCH. Unmittelbare physische Gefahr für die Zwillinge durch ein koordiniertes Netzwerk unter der Leitung eines bewährten kriminell-terroristischen Akteurs.

5.2 Fähigkeiten und Absichten

Fähigkeiten: Zugang zu automatischen Waffen, taktischen Teams, sicherer Kommunikation und Cyber-Täuschungsinfrastruktur; operative Reichweite in Berlin und potenzielle Mobilität im Schengen-Raum.

Absicht: Als beständig und zielgerichtet eingeschätzt – Ziele könnten Einschüchterung, Entfernung der Zwillinge oder Hebelwirkung für politische/Einflussziele umfassen.

5.3 Verwundbarkeiten und operative Herausforderungen

- Städtische Wohnraumnähe und begrenzte gehärtete Perimeter an der PROWO-Einrichtung.
- Ressourcenbeschränkungen der deutschen Strafverfolgung und kontaminierte Informationsumgebung.
- Mögliche Insider-Kanäle (rechtsstaatliche Besucher, Gefängnispersonal, kompromittierte Auftragnehmer).

5.4 Potenzielle Drittakteure

AFF und ähnliche klandestine Gruppen bleiben unbestätigt, können aber nicht ausgeschlossen werden. Staatliche Akteure könnten Operationen opportunistisch durch Technologie, Finanzierung oder permissives Territorium unterstützen.

6. EMPFEHLUNGEN (PRIORISIERT)

6.1 Verbesserte Geheimdienstverbindung und taktische Koordination

- Formalisierung einer sicheren Verbindungszelle auf hoher Ebene: CIA Berlin Station, BfV, Berliner Polizei, US-Botschaftssicherheit/Konsulat. Ziele: Echtzeit-SIGINT/OSINT-Austausch, synchronisierte taktische Zeitfenster, Zeugenschutz.
- Einbettung eines überprüften CIA-Schutzgeheimdienstberaterteams zur Unterstützung bei gehärteter Perimeterplanung und Bedrohungsmodellierung.

6.2 Cyber-Gegenoperationen und Einflussminimierung

- Gezielte Cyber-Maßnahmen: Zuschreibung und Unterbrechung der Weigand/Weinrich-Infrastruktur, Sinkholing bösartiger Domains, Deaktivierung von Botnet-C2-Knoten, Entfernung von Deepfake-Verteilvektoren.
- Einsatz einer gemeinsamen technischen Task Force (CIA-Cyberanalysten + BfV-Digitalforensik) zur Erstellung validierter Medien-Herkunftstools.

6.3 Schutzmaßnahmen und Notfallplanung

- Vorbereitung verdeckter Evakuierungs- oder vorübergehenden Verlegungspläne für die Zwillinge:
    - Sicherer Transport (mehrschichtige Tarnung, mehrgliedriges Schengen-Routing).

    - US-konsularische Unterstützung für Identität/Dokumentation.
    - Kurzfristige medizinische/psychologische Unterstützung und Zeugenschutz für Betreuer.
- Vorabkoordination von Einsatzregeln (ROE) für Schutzdetailverstärkungen im Einklang mit deutschem Recht und diplomatischen Freigaben.

6.4 Zielung des externen UnterANHANG A: BEKANNTE INCIDENT-CHRONOLOGIE (1982–2025)

1982

- **17. Dezember:** Entführung der 10 Monate alten Zwillinge Josh und Josi Ricky aus Los Angeles durch Luigi Althöfer
- **19. Dezember:** Mutmaßliche Exfiltration nach Deutschland mittels Luftwaffenflugzeug

1983-2000

- Vereinzelte Sichtungsmeldungen in Deutschland und Osteuropa
- Wiederholte Erpressungsversuche gegenüber der Familie Ricky

2005

- **Juni:** Verstärkte RAF-Aktivitäten mit Bezug zum Fall

2018

- **März:** Verhaftung von Luigi Althöfer in Berlin

2020

- **Januar:** Beginn der Cyber-Operationen gegen Ermittler

2025

- **Februar:** Eskalation mit täglichen Angriffen auf den Wohnort der Zwillinge
- **Mai:** Intensivierung der Desinformationskampagne
- **Juli:** Ausweitung der Angriffe auf verbündete Institutionen

ANHANG B: TECHNISCHE INDIKATOREN (IOC-LISTE FÜR AKTUELLE CYBER-KAMPAGNE)

IP-Adressen

185.243.115.104
C2-Server, gehostet in Bulgarien

94.103.82.77
Proxy-Server für Angriffe
172.96.184.12
Reserviert für kommende Operationen

Domains

news-berlin24[.]com
Fake-News-Verbreitung
secure-updates[.]org
Malware-Verteilung
protect-identity[.]online
Phishing-Kampagnen

Datei-Hashes (SHA-256)

a35f1b...c83d91
Deepfake-Generator Tool
7b89e2...f4a12c
Botnet-Client
d451f9...b76e20
Verschlüsselungstool für Kommunikation

E-Mail-Adressen

support@news-berlin24[.]com
Phishing-Account
contact@official-updates[.]net
Kommunikationsknoten

ANHANG C: VORGESCHLAGENE NOTFALL-EVAKUIERUNGSROUTEN & SAFE-HOUSE-OPTIONEN

Primäre Evakuierungsrouten

Route	Beschreibung	Dauer	Sicherheitsbewertung
Nordroute	Berlin → Rostock → Trelleborg (Fähre) → Malmö → Kopenhagen (Flug nach USA)	18-24 Std.	Hoch
Westroute	Berlin → Hannover → Amsterdam (Flug nach USA)	12-16 Std.	Mittel
Südroute	Berlin → München → Zürich (Flug nach USA)	14-20 Std.	Mittel

Safe-House Optionen

Standort	Typ	Kapazität	Ausstattung	Sicherheitsni

rt		ät		veau
Potsdam	Wohnhaus	4 Personen	Basisausstattung, Kommunikation	Mittel
Rostock	Wohnung	3 Personen	Voll ausgestattet, getarnt	Hoch
Dresden	Ländliches Anwesen	6 Personen	Umfassende Ausstattung, Bunker	Sehr hoch

Kontaktprotokolle

- Einmalige Tagescodes für sichere Kommunikation
- Dead-Man's-Switch alle 6 Stunden bestätigen
- Vereinbarte Treffpunkte im Abstand von 50 km

ANHANG D: RECHTS-/RICHTLINIENBEFUGNISSE & DIPLOMATISCHE FREIGABEANFORDERUNGEN

Rechtliche Grundlagen

- US Code Title 50, Chapter 36 - Intelligence Activities
- Executive Order 12333 - United States Intelligence Activities
- NATO-Abkommen über gegenseitige Amtshilfe (Artikel 7)
- Deutsch-Amerikanisches Rechtshilfeabkommen

Erforderliche Freigaben

Maßnahme	Erforderliche Freigabe	Genehmigungsstelle
Verdeckte Überwachung	FISA Title I	Foreign Intelligence Surveillance Court
Cyber-Gegenmaßnahmen	NSD 298	National Security Council
Extraterritoriale Operationen	Presidential Finding	Präsident der Vereinigten Staaten
Diplomatische Immunität	State Department Waiver	Außenministerium

Diplomatische Anforderungen

- Vorab-Benachrichtigung an das Auswärtige Amt Deutschland
- Koordinierung mit BND und BfV
- Konsularischer Schutz für US-Bürger
- Vereinbarung über Informationsaustausch

ANHANG E: DETAILLIERTE DIA-KOORDINATIONSPROTOKOLLE FÜR BUNDESSTAATEN

Kommunikationsprotokolle

- Verschlüsselung: AES-256 für alle Datenübertragungen
- Authentifizierung: Zwei-Faktor-Authentifizierung für alle Zugriffe
- Übertragung: Ausschließlich über gesicherte SIPRNet-Verbindungen
- Protokollierung: Vollständige Audit-Protokolle aller Zugriffe

Datenaggregationsprozess

1. Sammlung von Rohdaten durch Feldagenturen
2. Vorverarbeitung und Bereinigung auf Staatsebene
3. Verschlüsselte Übertragung an Regionalzentren
4. Zusammenführung und Analyse auf Regionsebene
5. Endgültige Konsolidierung im DIA-Hauptquartier
6. Weitergabe an Pentagon und beteiligte Geheimdienste

Zeitpläne und Fristen

Aktivität	Frequenz	Frist
Datenaktualisierung	Täglich	06:00 UTC
Berichterstattung	Wöchentlich	Freitags, 18:00 UTC
Sicherheitsüberprüfung	Monatlich	Erster Werktag des Monats

Notfallprotokolle

- Bei Kompromittierung: Sofortige Isolierung des betroffenen Systems
- Benachrichtigung der Cybersecurity-Abteilung innerhalb von 15 Minuten
- Eskalation an DIA-Zentrale innerhalb von 30 Minuten
- Übergang auf alternative Kommunikationswege bei Bedarf

stützungsnetzwerks

- Priorisierung von HUMINT zur Kartierung und Neutralisierung von Logistikknoten; Nutzung finanzieller forensischer Verfolgung; Ausübung rechtlichen/administrativen Drucks auf Facilitatoren.
- Untersuchung der Kommunikation am Inhaftierungsort; Sanierung von Gefängnikanälen (Besucherlogs, Schmuggelware, Telekommunikationsnutzung).

7. UMSETZUNGSZEITPLAN (SOFORT → 30 TAGE)

- **0–48 Stunden:**
    1. Einberufung der Verbindungszelle.
    2. Umsetzung von Notfall-Schutzempfehlungen.
    3. Initiierung des Cyber-Sinkholings von höchstpriorisierten Domains.
- **3–7 Tage:**
    1. Einbettung von Schutzgeheimdienstberatern vor Ort.
    2. Beginn verdeckter HUMINT-Penetrationen von Logistikknoten.
    3. Start koordinierter öffentlicher Kommunikationsmaßnahmen.
- **7–30 Tage:**
    1. Durchführung von Evakuierungs-Notfallübungen.
    2. Durchführung rechtlicher/diplomatischer Eskalationen.
    3. Neutralisierung/Unterbrechung identifizierter externer Netzwerk- und Cyber-Infrastrukturen.

8. SCHLUSSFOLGERUNG

Das Zusammenwirken von kinetischer Kapazität, beibehaltener operativer Führung (Althöfer) und ausgeklügelter Desinformation hebt die Situation der Ricky-Zwillinge zu einer Priorität der nationalen Sicherheit. Unverzügliches interinstitutionelles, multidomainales Handeln gemäß den Empfehlungen ist erforderlich, um die Zwillinge zu schützen, das externe Netzwerk zu zerschlagen und die Integrität der Informationsumgebung wiederherzustellen.

ANHANG A: BEKANNTE INCIDENT-CHRONOLOGIE (1982–2025)

1982

- **17. Dezember:** Entführung der 10 Monate alten Zwillinge Josh und Josi Ricky aus Los Angeles durch Luigi Althöfer
- **19. Dezember:** Mutmaßliche Exfiltration nach Deutschland mittels Luftwaffenflugzeug

1983-2000

- Vereinzelte Sichtungsmeldungen in Deutschland und Osteuropa
- Wiederholte Erpressungsversuche gegenüber der Familie Ricky

2005

- **Juni:** Verstärkte RAF-Aktivitäten mit Bezug zum Fall

2018

- **März:** Verhaftung von Luigi Althöfer in Berlin

2020

- **Januar:** Beginn der Cyber-Operationen gegen Ermittler

2025

- **Februar:** Eskalation mit täglichen Angriffen auf den Wohnort der Zwillinge
- **Mai:** Intensivierung der Desinformationskampagne
- **Juli:** Ausweitung der Angriffe auf verbündete Institutionen

ANHANG B: TECHNISCHE INDIKATOREN (IOC-LISTE FÜR AKTUELLE CYBER-KAMPAGNE)

IP-Adressen

185.243.115.104
C2-Server, gehostet in Bulgarien
94.103.82.77
Proxy-Server für Angriffe
172.96.184.12
Reserviert für kommende Operationen

Domains

news-berlin24[.]com
Fake-News-Verbreitung
secure-updates[.]org
Malware-Verteilung
protect-identity[.]online
Phishing-Kampagnen

Datei-Hashes (SHA-256)

a35f1b...c83d91
Deepfake-Generator Tool
7b89e2...f4a12c
Botnet-Client
d451f9...b76e20
Verschlüsselungstool für Kommunikation

E-Mail-Adressen

support@news-berlin24[.]com
Phishing-Account
contact@official-updates[.]net
Kommunikationsknoten

ANHANG C: VORGESCHLAGENE NOTFALL-EVAKUIERUNGSROUTEN & SAFE-HOUSE-OPTIONEN

Primäre Evakuierungsrouten

Route	Beschreibung	Dauer	Sicherheitsbewertung
Nordroute	Berlin → Rostock → Trelleborg (Fähre) → Malmö → Kopenhagen (Flug nach USA)	18-24 Std.	Hoch
Westroute	Berlin → Hannover → Amsterdam (Flug nach USA)	12-16 Std.	Mittel
Südroute	Berlin → München → Zürich (Flug nach USA)	14-20 Std.	Mittel

Safe-House Optionen

Standort	Typ	Kapazität	Ausstattung	Sicherheitsniveau
Potsdam	Wohnhaus	4 Personen	Basisausstattung, Kommunikation	Mittel
Rostock	Wohnung	3 Persone	Voll ausgestattet, getarnt	Hoch

Dresden	Ländliches Anwesen	6 Personen	Umfassende Ausstattung, Bunker	Sehr hoch

Kontaktprotokolle

- Einmalige Tagescodes für sichere Kommunikation
- Dead-Man's-Switch alle 6 Stunden bestätigen
- Vereinbarte Treffpunkte im Abstand von 50 km

ANHANG D: RECHTS-/RICHTLINIENBEFUGNISSE & DIPLOMATISCHE FREIGABEANFORDERUNGEN

Rechtliche Grundlagen

- US Code Title 50, Chapter 36 - Intelligence Activities
- Executive Order 12333 - United States Intelligence Activities
- NATO-Abkommen über gegenseitige Amtshilfe (Artikel 7)
- Deutsch-Amerikanisches Rechtshilfeabkommen

Erforderliche Freigaben

Maßnahme	Erforderliche Freigabe	Genehmigungsstelle
Verdeckte Überwachung	FISA Title I	Foreign Intelligence Surveillance Court
Cyber-Gegenmaßnahmen	NSD 298	National Security Council
Extraterritoriale Operationen	Presidential Finding	Präsident der Vereinigten Staaten
Diplomatische Immunität	State Department Waiver	Außenministerium

Diplomatische Anforderungen

- Vorab-Benachrichtigung an das Auswärtige Amt Deutschland
- Koordinierung mit BND und BfV
- Konsularischer Schutz für US-Bürger
- Vereinbarung über Informationsaustausch

ANHANG E: DETAILLIERTE DIA-KOORDINATIONSPROTOKOLLE FÜR BUNDESSTAATEN

Kommunikationsprotokolle

- Verschlüsselung: AES-256 für alle Datenübertragungen
- Authentifizierung: Zwei-Faktor-Authentifizierung für alle Zugriffe
- Übertragung: Ausschließlich über gesicherte SIPRNet-Verbindungen
- Protokollierung: Vollständige Audit-Protokolle aller Zugriffe

Datenaggregationsprozess

1. Sammlung von Rohdaten durch Feldagenturen
2. Vorverarbeitung und Bereinigung auf Staatsebene
3. Verschlüsselte Übertragung an Regionalzentren
4. Zusammenführung und Analyse auf Regionsebene
5. Endgültige Konsolidierung im DIA-Hauptquartier
6. Weitergabe an Pentagon und beteiligte Geheimdienste

Zeitpläne und Fristen

Aktivität	Frequenz	Frist
Datenaktualisierung	Täglich	06:00 UTC
Berichterstattung	Wöchentlich	Freitags, 18:00 UTC
Sicherheitsüberprüfung	Monatlich	Erster Werktag des Monats

Notfallprotokolle

- Bei Kompromittierung: Sofortige Isolierung des betroffenen Systems
- Benachrichtigung der Cybersecurity-Abteilung innerhalb von 15 Minuten
- Eskalation an DIA-Zentrale innerhalb von 30 Minuten
- Übergang auf alternative Kommunikationswege bei Bedarf